Operating System Fundamentals

Module 3:

Users and Groups

Agenda

- Users
- Groups
- Privileges
- Windows Implementation
  - Access Control List
  - Local Users and Groups
  - Active Directory
  - Policies

Users

- Why?
  - Security
  - Multiple Use PC
  - Profiles
    - Single person with many profiles
    - Application specific profile
- Security rights or privileges assigned

Groups

- Collection of Users with equal rights
- Easier to manage security for a group at a time
- User may be member of more than one group
  - Security rights assigned to group is inherited by user
- Groups may already exist with profiles for your convenience

Privileges

- Normally assigned to files or folders (directories)
- Defines
  - What can be accessed
  - How it can be accessed (e.g. read, write, execute)
- Assigned to users or groups

Tip

- Administrator (or Root) account should NEVER be used for normal activity – reserve it for emergency recovery
- Create another account and make it a member of the Administrative group – use that one instead
- Save the original administrator password in a "locked vault", where only a few people know how to access it

Windows Implementation

- Everything in Windows is an object with an Access Control List (ACL)
- ACL is a collection of Access Control Entries
  - Specifies who has access (or denial)
  - Specifies specific permissions (or denials)
- Controlled by API (program)
- User Interface provided for management of most objects
  - Need permission to change it ☺

- Make sure Control Panel is *not* viewed by Category
- Accessed through Control Panel->Administrative Tools
- Manage users and groups for the local computer
- If you need to share resources in a workgroup, all computers MUST have the same users and passwords

Local Users and Groups

Examples of Secured Objects

- Files
  - Data
  - Programs
- Directories
- Shared Resources
  - Directories
  - Printers

Securing Shared Resources

- Two step process to share directories
  - Permit access to object
  - Permit access to share
- Use UNC name to access the share
  - Ex: **\\server\share\path**

Workgroup

- Peer-to-peer network
- For secured access, user id’s and passwords need to be duplicated across computers
- Basis of Windows 7/8 Homegroup feature

Central Server

- Central list of users, groups and shared resources
  - Managed centrally
- Better security management than Workgroup model
- Good for small networks where only 1 server is sufficient

Active Directory

- Central list of users, groups and shared resources
  - Managed centrally
- Uses the domain model
  - Single Domain Controller per domain
  - Multiple Backup Domain Controllers possible
- Enables users to log in anywhere in the "Enterprise"
  - Validates against the Active Directory

Policies

- Policies are "business rules" and may not be specific to an object in the system
- Common policies revolve around
  - Passwords (Security Policies)
  - Windows desktop settings (Group Policies)
- Data saved in the Registry
  - “regedit” or “regedt32” at the command line
  - USE EXTREME CAUTION WHEN CHANGING THE REGISTRY

Policies

- To manage local group policies
  - Start mmc (in command line)
  - Use File->Add/Remove Snap-in
  - Select Group Policy Object
- To manage security
  - Use Group Policy Add-in for mmc
    or
  - Go to Control Panel->Administrative Tools
  - Select Local Security Policy
- In a Domain environment
  - Choices are similar but controlled centrally

Tip

- Installing software on local machine is a local permission
- In Active Directory, all Domain Administrators are Local Administrators
- If you allow users to install software locally, make the user (or Domain Users) part of the Local Administrators group