LAB 5. Group Policy

I. Yêu cầu:

- Hiểu được khái niệm Group Policy
- Nắm được các chính sách bảo mật trên máy tính cục bộ.
- Sử dụng Local Computer Policy cấu hình được một số policy cơ bản.

II. Tóm tắt lý thuyết:

- Group Policy được dùng để quản lý cấu hình phần lớn các thành phần và đặc trưng của Windows, liên quan đến việc bảo mật và cài đặt phần mềm. Group Policy cho phép quản lý các thay đổi và cấu hình ở cấp độ user hay máy tính tại điểm quản trị tập trung. Hàng ngàn thiết đặt cấu hình có thể được quản lý với Group Policy.
- Có thể cấu hình Group Policy trên mô hình quản trị miền Active Directory bằng Domain based GPO – Group Policy Object Editor hay cấu hình Local GPO bằng Local Computer Policy, chỉ có phạm vi áp dụng trên máy tính cục bộ.
- Với Group Policy, bạn có thể:
  - ✓ Triển khai phần mềm ứng dụng
  - ✓ Gán các quyền hệ thống cho người dùng
  - ✓ Giới hạn những ứng dụng mà người dùng được phép thi hành
  - ✓ Kiểm soát các thiết lập hệ thống
  - ✓ Kiểm soát các kịch bản đăng nhập, đăng xuất, khởi động và tắt máy.
  - ✓ Đơn giản hóa và hạn chế các chương trình
  - ✓ Hạn chế tổng quát màn hình Desktop của người dùng
- Group Policy có 2 nhánh chính:
  - Computer configuration: áp dụng cho toàn bộ user trên máy
    - Software settings: triển khai phần mềm ứng dụng
    - Windows settings: quản lý việc khởi động, shutdown, sử dụng tài khoản, mật khẩu.
    - Administrative Template: cấu hình hệ thống, các thành phần cài đặt trong windows
  - User Configuration: cấu hình theo user
    - Windows settings: quản lý việc logon / logoff, sử dụng tài khoản, mật khẩu.
    - Administrative Template: tương tự nhánh computer configuration. Chỉ có một số ít khác biệt về các chính sách.
- Mỗi policy thông thường có 3 tùy chọn cấu hình:
  - Not configured: không định cấu hình cho chính sách
  - Enable: kích hoạt chính sách
  - Disable: vô hiệu hóa chính sách

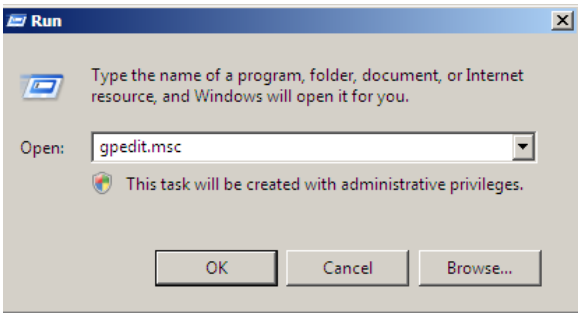
- Lệnh sử dụng: gpedit.msc

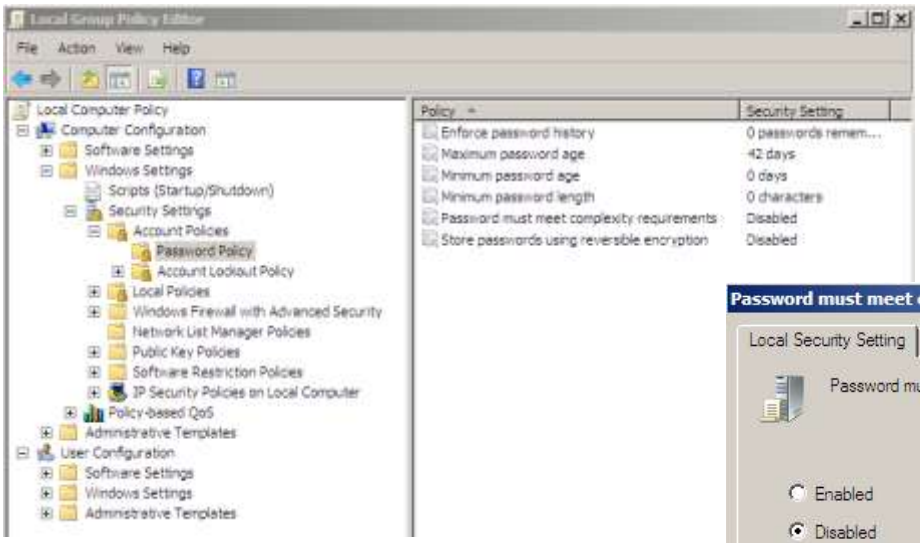
III. Chuẩn bị

- Bài LAB sử dụng 2 máy: 1 máy XP và 1 máy Windows Server 2008 thuộc mạng 192.168.10.0
- Bảo đảm đường truyền đã thông
- Đổi password của Administrator máy XP là xp2@123
- Đổi password của Administrator máy Windows Server 2008 là win2k8@123
- Tạo các user cục bộ: gv1 và gv2 thuộc group giangvien, sv1 và sv2 thuộc group sinhvien

IV. Triển khai

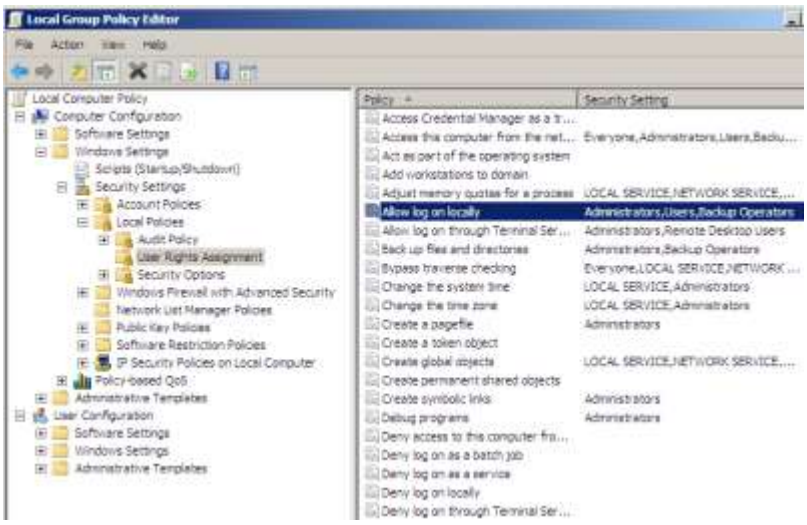
1. Bỏ giới hạn password, cho phép tạo user với password trống (Password Policy)
   Chọn Start > Run



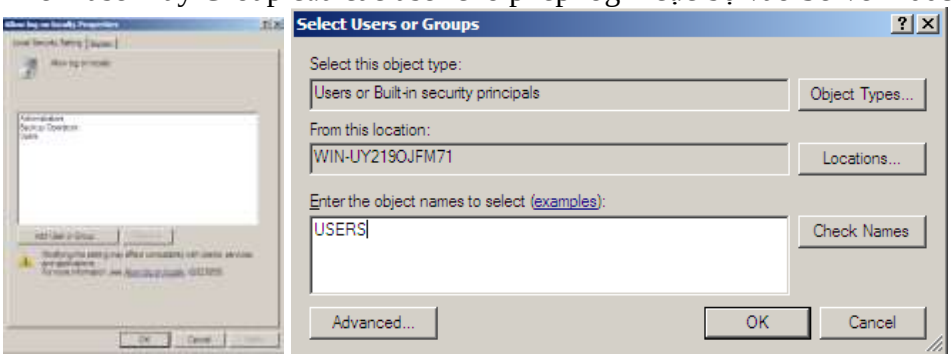


   Cập nhật lại chính sách bảo mật: Start > Run > Cmd > gpupdate /force.
   Thực hiện tạo user SV3 với password trống.

2. Cho phép user tạo mới đăng nhập cục bộ vào Server 2008 (Allow logon locally)
   Chọn Start > Run > gpedit.msc

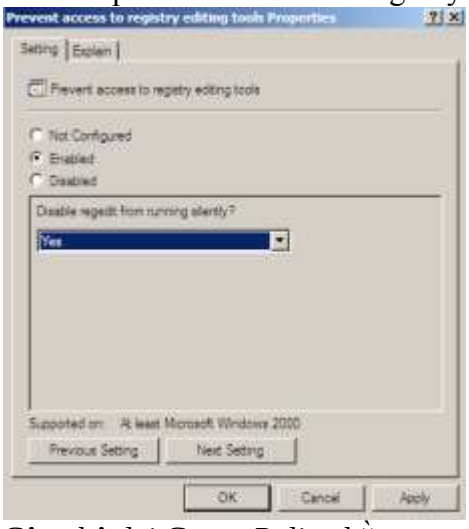


Thêm user hay Group của các user cho phép login cục bộ vào Server 2008



Cập nhật lại chính sách bảo mật cục bộ: gpupdate/force
Tạo User mới SV4, logoff Administrator, thử logon bằng SV4.

3. Chặn thay đổi Registry bằng GPO
   Chọn Start > Run > gpedit.msc
   Tìm theo đường dẫn User Configuration Policies > Administrative Template > System.
   Click đúp Prevent access to registry editing tools



Cập nhật lại Group Policy bằng gpupdate/force.

V. Bài tập

Cấu hình các chính sách bảo mật cục bộ sau trên máy XP và máy Windows Server 2008

1. Cho phép user SV1 có thể thay đổi giờ hệ thống máy tính, nhưng SV2 thì không *(Change the system time)*
2. Không giới hạn số ngày có hiệu lực của mật khẩu người dùng *(Maximum password age)*
3. Cho phép user gv1 shutdown hệ thống, nhưng các sinh viên sv1, sv2 thì không (*Shutdown the system*)
4. Cho phép user cài đặt các trình điều khiển máy in *(Devices: Prevent users from installing printer drivers)*
5. Cấm truy xuất ghi dữ liệu ra USB (*Removable Disks: Deny write access*)
6. Cấm truy xuất đọc CD/DVD (*CD/DVD: Deny read access*)
7. Tắt âm thanh khi khởi động Windows (*Turn off Windows Startup Sound)*
8. Làm mất biểu tượng Recycle Bin trên Desktop (*Remove Recycle Bin from desktop)*
9. Gỡ bỏ tên user đang logon khỏi menu Start (*Remove user name from Start Menu*)
10. Tắt kết nối tới Projector mạng (*Turn off Connect to a Network Projector*)
11. Ngăn chặn các user share file trong profile của họ (*Prevent users from sharing files within their profile*)
12. Làm biến mất Control Panel (*Prohibit access to the Control Panel*)
13. Tắt chế độ AutoPlay của CDROM (*Turn off Autoplay*)
14. Ngăn chặn user thêm hay thay đổi màn hình nền của Desktop (*Prevent changing wallpaper)*
15. Đổi tên user Guest (*Accounts: Rename guest account*)
16. Cho phép ghi log truy xuất các đối tượng hệ thống global (*Audit: Audit the access of global system objects*)
17. Cho phép xóa pagefile nhớ ảo khi hệ thống shutdown (*Shutdown: Clear virtual memory pagefile*)
18. Bật ghi log việc user truy xuất 1 đối tượng như tập tin, thư mục, khóa registry, máy in, … thành công / thất bại. (*audit object access*)
19. Cấm sv2 logon cục bộ vào máy tính (*deny log on locally*)
20. Cho phép quản lý hạn ngạch đĩa trên các volume NTFS và ngăn chặn user thay đổi cấu hình (*Enable disk quotas*)
21. Ngăn chặn người dùng sử dụng Add or Remove Programs (*Remove Add or Remove Programs*)
22. Ẩn tab Screen Saver (*Hide Screen Saver tab*)
23. Ngăn chặn việc gỡ bỏ máy in (*Prevent deletion of printers)*
24. Cấm cấu hình các thuộc tính TCP/IP nâng cao (*Prohibit TCP/IP advanced configuration*)
25. Ẩn biểu tượng My Computer trên Desktop (*Remove Computer icon on the Desktop)*
26. Hạn chế truy xuất phần mềm: phần mềm sẽ không chạy nếu không có quyền truy xuất của user (*Security levels: Disallowed*)
27. Không cho chạy chương trình Calculator (*Don't run specified Windows applications*)

28. Ngăn chặn Windows tự tìm các bản update trên internet (*Windows Automatic Updates*)
29. Ngăn chặn truy xuất tới Command prompt (*Prevent access to the command prompt*)
30. Hiển thị câu chào "Welcome to my computer!" khi khởi động máy tính và câu "Good bye. See you again." Khi shutdown máy tính (*Scripts(Startup/Shutdown)*)