

LAB 6. Registry

I. Yêu cầu:

- Hiểu được khái niệm Registry
- Nắm được các thiết đặt cấu hình registry thông dụng.
- Cấu hình được registry bằng dòng lệnh.

II. Tóm tắt lý thuyết:

Registry là một cơ sở dữ liệu dùng để lưu trữ thông số kỹ thuật của Windows. Cơ sở dữ liệu của nó lưu hầu hết các thiết đặt quan trọng nhất giúp hệ điều hành và các ứng dụng hoạt động. Nắm rõ registry sẽ giúp bạn tiến xa hơn trong kỹ thuật lập trình trên nền Windows, cách bảo mật, cracking, hacking.

Các nhóm khóa chính của Registry:

- HKEY_Classes_Root: thông tin chung hệ thống
- HKEY_Current_User: thông tin user đang logon
- HKEY_Local_Machine: thông tin hệ thống, phần cứng, phần mềm
- HKEY_Users: thông tin user
- HKEY_Current_Config: thông tin phần cứng đang dùng
- HKEY_Dyn_Data: một phần của HKEY_Local_Machine

* **Các lệnh sử dụng:** reg.exe

Cú pháp:

- Truy vấn thông tin registry: reg query
- Thêm và xóa các nội dung registry: reg add keyname hay reg delete keyname
- Sao chép các nội dung registry: reg copy keyname1 keyname2
- Export nội dung registry: reg export keyname filename
- Import nội dung registry: reg import filename
- Lưu và phục hồi các nội dung registry: reg save keyname filename, reg restore keyname filename

III. Chuẩn bị

- Bài LAB sử dụng 1 máy Windows Server 2008 thuộc mạng 192.168.10.0
- Đổi password của Administrator máy Windows Server 2008 là win2k8@123

IV. Triển khai

1. Kiểm tra các khóa tắt share mặc định:

reg query HKLM\system\currentcontrolset\services\lanmanserver\parameters /s

```
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\lanmanserver\parameters
EnableAuthenticateUserSharing REG_DWORD 0x0
ServiceDllUnloadOnStop REG_DWORD 0x1
ServiceDll REG_EXPAND_SZ %SystemRoot%\system32\svrsvc.dll
NullSessionPipes REG_MULTI_SZ
autodisconnect REG_DWORD 0xf
enableforcedlogoff REG_DWORD 0x1
enablesecuritysignature REG_DWORD 0x0
requiresecuritysignature REG_DWORD 0x0
restrictnullsessaccess REG_DWORD 0x1
Lmannounce REG_DWORD 0x0
Size REG_DWORD 0x3
AdjustedNullSessionPipes REG_DWORD 0x3
AutoShareServer REG_DWORD 0x0
AutoShareWks REG_DWORD 0x0
Guid REG_BINARY 282ACAF733C38F4DB9E398DF8EBC83E6
```

2. Thay đổi thông số cảnh báo không gian đĩa cứng là 5%

reg add HKLM\system\currentcontrolset\services\lanmanserver\parameters
/v diskspacethreshold /t reg_dword /d 5

V. Bài tập

1. Tắt Settings của Display trong Control Panel
2. Tắt mục ScreenSaver của Display trong Control Panel
3. Không cho thay đổi hình nền, màu nền của Desktop
4. Điều khiển chế độ tự động mở đĩa CD khi đưa đĩa vào ổ.
5. Ẩn mục Security trong Windows Explorer
6. Không cho phép Internet Explorer tải file từ internet về.
7. Không cho phép truy xuất file từ một đường dẫn internet.
8. Xóa những địa chỉ web bạn đã vào.
9. Hiện thị nút Shutdown trên hộp thoại Dialog
10. Cho phép user tự động logon sau khi khởi động
11. Ẩn nút Change Password
12. Không cho phép hiện tên người dùng cuối cùng
13. Đặt độ dài tối thiểu của password là 0
14. Hiện thị thông tin về CPU
15. Ẩn biểu tượng My Computer trên Start Menu và Desktop
16. Tắt cửa sổ Task Manager
17. Không cho phép dùng công cụ Registry Editor để chỉnh sửa Registry
18. Tắt lệnh Shutdown
19. Xóa Page File khi tắt máy
20. Hạn chế một số ứng dụng mà người dùng có thể chạy
21. Xóa các tài liệu đã làm việc khi tắt Windows
22. Không cho hiện thị danh sách các tài liệu đã truy cập trên Start Menu

23. Không cho hiện menu Context khi nhấn chuột phải trên Taskbar
24. Ngăn quyền truy cập đĩa CDROM
25. Vô hiệu hóa chức năng Windows Update
26. Vô hiệu hóa tất cả chương trình khởi động cùng Windows đã đăng ký trong registry
27. Hiện thị hộp thông báo trước khi logon “Welcome to my computer!”
28. Không cho phép hiện tên người dùng cuối cùng trong hộp thoại logon
29. Yêu cầu password khi unlock máy hay thoát khỏi Screen Saver
30. Ẩn menu Folder options trong Windows Explorer

*** Tài liệu tham khảo:** Windows Registry