
Start -> (type in) Active Directory Users and Computers
Expand the server (something.local) and click “Users”
Right click in the white part of the user pane and hit new -> user
Enter name and password (from password sheet, dummy)
Uncheck first box (change pw on login or whatever)
After you finish adding this user: Right click and select properties
Go to “Member of” tab
Click add -> advanced -> find now
Select Account Operators, Administrators, DHCP Administrators, DNS Admins, Domain Admins, Enterprise Admins, Event Log Readers, Group Policy Creator Owners, Performance Log Users, Performance monitor users, Print Operators, Remote Desktop Users, Schema Admin, Server Operator.
OK, OK, Apply
Do it again, but with a different username and password
Log out, log in to new account
Disable regular admin account and any other dangerous accounts

---

XP/2k3 then PATCH MS08_067
Block ports 139 & 445 in the windows firewall

Vista/7/2k8 then PATCH MS09_050
Block ports 139 & 445 in the windows firewall

1. Click **Start**, click **Run**, type **Regedit** in the **Open** box, and then click **OK**.
2. Locate and then click the following registry subkey:
3.
4. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
5. Click **LanmanServer**.
6. Click **Parameters**.
7. Right-click to add a new **DWORD (32 bit) Value**.
8. Enter **smb2** in the **Name** data field, and change the **Value** data field to **0**.
9. Exit.
10. Restart the "Server" service by performing one of the following:
11.
12. - Open up the computer management MMC, navigate to **Services and Applications**, click **Services**, right-click the **Server** service name and click **Restart**. Answer **Yes** in the pop-up menu.
13.
14. - From a command prompt and with administrator privileges, type **net stop server** and then **net start server**.

Disable Powershell
Start, Type in: Turn Windows Features on or off
Disable powershell

Audit Policy
Click start, type in: Group Policy Management
Open: Forest -> Domain -> Server -> Server ->Group Policy Objects -> Default Domain Policy,
Right click, edit

Account Login:
Audit Credential Validation: Failure
Audit other account logon events: Success and failure

Account Management:
Audit Security Group Management: Success and failure
Audit User Account Management: Success and failure
Login/Logoff
Audit Account Lockout: Success and failure
Audit logoff: Success and failure
Audit logon: Failure
Audit other logon/logoff events: Success and failure
Audit Special Logon: Success and failure

Object Access:
Audit Kernel Object: Success and failure
Audit Other Object Access Events: Success and failure
Audit Registry Properties: Success and failure
Audit SAM: Failure

Policy Change:
Audit Audit Policy Change: Success and failure
Audit Authentication Policy Change: Success and failure
Audit Authorization Policy: Success and failure
Audit other policy change events: Success and failure

Privilege Use
Audit Non Sensitive Privilege Use: Success and failure
Audit Other Privilege Use Events: Success and failure
Audit Sensitive Privilege Use: Success and failure

System
Audit Other System Events: Success and Failure
Audit Security System Extension: Success and failure
Audit System Integrity: Failure

Start > Run type in eventvwr

Windows security compliance management toolkit
goo.gl/qO7y49
Microsoft baseline security analyzer (MBSA)
goo.gl/GJ8CVp
SCW (security configuration wizard)
http://securitywing.com/windows-2008-server-security-hardening-with-automated-tools/

Disable LM Hashing

1. In Group Policy, expand Computer Configuration, expand Windows Settings, expand Security Settings, expand Local Policies, and then click Security Options.
2. In the list of available policies, double-click Network security: Do not store LAN Manager hash value on next password change.
3. Click Enabled, and then click OK.

Use SYSKEY to encrypt SAM file

1. Type SYSKEY into the textbox on the start menu. Click OK at the UAC prompt.
2. Select the Encryption Enabled Option.
3. Select the Password Startup Option. ...
4. Reboot the computer.

Forensics, incident reporting

Display a local share
NET SHARE sharename

Display a list of computers in the current domain.
NET VIEW

To see a list of shares on a remote computer
NET VIEW \\ComputerName

To see a list of all shares in the domain:
NET VIEW /DOMAIN

To see a list of shares on a different domain
NET VIEW /DOMAIN:domainname

To see a list of shares on a remote Netware computer
NET VIEW /NETWORK:NW [\\ComputerName]

Create a new local file share
NET SHARE sharename=drive:path /REMARK:"text" [/CACHE:Manual | Automatic | No]

Limit the number of users who can connect to a share
NET SHARE sharename /USERS:number /REMARK:"text"

Remove any limit on the number of users who can connect to a share
NET SHARE sharename /UNLIMITED /REMARK:"text"

Delete a share
NET SHARE {sharename | devicename | drive:path} /DELETE

Delete all shares that apply to a given device
NET SHARE devicename /DELETE
In this case the devicename can be a printer (Lpt1) or a pathname (C:\Docs\)

Join a file share (Drive MAP)
NET USE

Display all the open shared files on a server and the lock-id
NET FILE

Close a shared file (disconnect other users and remove file locks)
NET FILE id /CLOSE

List all sessions connected to this machine
NET SESSION

List sessions from a given machine
NET SESSION \\ComputerName

Disconnect all sessions connected to this machine
NET SESSION /DELETE

Disconnect all sessions connected to this machine (without any prompts)
NET SESSION /DELETE /y

Disconnect sessions from a given machine
NET SESSION \\ComputerName /DELETE

Windows Software for the PAK:
goo.gl/APTn3m Process Hacker
goo.gl/wV47eJ / TCPView
goo.gl/baUqtW / Process Explorer
goo.gl/0QjkQz / Putty
http://www.wireshark.org / Wireshark
goo.gl/WG35NT / autoruns

Network security: LAN Manager authentication level - Send NTLMv2 response only\refuse NTLM & LM
GPO_name\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options
Level 5 - DC refuses LM and NTLM responses (accepts only NTLMv2)

Network access: Do not allow anonymous enumeration of SAM accounts and shares - Enabled
&
Network access: Do not allow anonymous enumeration of SAM accounts - Enabled
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa registry subkey.
RestrictAnonymousSAM

Network access: Allow anonymous SID/name translation - Disabled

Interactive logon: Message text for users attempting to log on - sometimes an inject
goo.gl/4N9Oy7

c:\\windows\system32\config\Sec.Event.Evt contains the trace of an attacker's brute-force attempts