Windows 2003 Server Baseline v1.1

Before the installation, make sure you have the server disconnected from the network or behind a firewall on an IP address that has all incoming ports blocked. This is important for security. Until you have applied all updates and turned off all unnecessary services, the machine is vulnerable.

When you first boot from the cd some drivers will be loaded.

Next you will see a screen with "Welcome to Setup". Press enter to install windows.

The next page is the EULA; press F8 to agree

The next step is the drive partitioning. If the server only has one drive, partition it so the system has one partition and the data has one. The minimum required space is approximately between 1.25GB and 2GBaccording to the Getting started guide

A 12 GB partition for the system drive "c:" should be sufficient for the OS, future updates and swap file(depending on how much RAM is installed) and is the default unless the customer wants a different layout of the partitions.
So, create at least a 12 GB partition for the system and a second partition with the rest. After assigning the partitions, press enter to continue.

Next, format the drive using the NTFS file system, which is the third option. After it has finished formatting the drive, Windows is going to copy system files, collect information and install windows. Each step may take several minutes.

The next step is the "Regional and Language options". Set the language to English (United States) and the location United States, with a US keyboard.

Enter the Name and Organization.
Enter the product key.
Enter the computer name and administrator password.
Set the date and time.

Now it will continue with the automated part of the installation.

Remove the cd and reboot as directed. The base install is done.

Once the machine has rebooted, log in as the administrator to Install and uninstall some windows components. Start by going to the following:
Start->Control Panel->Add or Remove Programs
select Add/Remove Windows Components

The default values might differ between the various Windows Server 2003 versions. In the web edition, there is one service that should be disabled, as shown below:

Select Application Server and click details
Internet Information Server IIS
World Wide Web Service
De-select Remote Administration(HTML)

Before you can connect to the network you may have to use the Internet Connection Wizard, open it as shown below and follow the steps.
Start->Control Panel->Network Connections->Local Area Connections->New

Configure the network as follows:
Start->Control Panel->Network Connections->Local Area Connection
Select properties.
Un-check but do not un-install "File and printer sharing for Microsoft Networks".

Connect the server to a network that is behind a firewall:
Select Internet Protocol(TCP/IP) and click properties.
Configure the network card with an ip address that has all incoming ports blocked in the firewall, add dns, gateway and netmask.

Install all updates from windows updates:
Start->All Programs->Windows Update
Follow the instructions,

When all updates are done it, activate windows:
Click on the "Keys" in the lower right corner or
Start->All Programs->Accessories->System Tools->Activate Windows.
Select the first option,"Yes, let's activate windows over the internet now."
Select the secont option,"No, I don't want to register now; let's just activate Windows" and click next, then click finish when it acknowledges completion.

Enable Terminal Services for remote administration mode:
Click Start and select properties for My Computer
At the bottom of the Remote tab check the
box to "Allow users to connect to this computer"
Verify that you can access the server through Remote Desktop.

Disable all unnecessary services.

Next, disable TCP/IP NetBIOS port 137,138,139:
Open the Control Panel select Network Connections and select properties
go to properties for Internet Protocol (TCP/IP).
Click on the Advanced button and go to the WINS tab.
select Disable Netbios over TCP/IP

Open services under Administrative tools. and disable TCP/IP NetBIOS helper.

Disable NetBT port 445. This requires a reboot to take effect.

Open the Registry Editor and locate the following Key
HKLM\System\CurrentControlSet\Services\NetBT\Parameters.
In the right-hand side of the window find the option called TransportBindName.
Double click that value, and then delete the default value \Device\, giving it a blank value. Close the registry editor. Reboot your computer.
If you need the server to listen to port 445 again just do the reverse
and fill in this value for the registry key Value name: TransportBindName
Value data: \Device\

Open Services "Start->Administrative Tools->Services". and disable all additional unnecessary services Some of the following might be disabled by default:

Alerter
ClipBook
Computer Browser
DHCP Client
Distributed File System
Distributed Link Tracking Client
Distributed Link Tracking Server
Human Interface Device
IMAPI CD-BurningCOM Service
Indexing Service
Intersite Messaging
IpSEC services
Kerberos Key Distribution Center
Licence Logging
Messenger
Net Logon
NetMeeting Remote Desktop Sharing
Network DDE
Network DDE DSDM
Portable Media Serial Number
PrintSpooler
Remote Access Auto Connection Manager
Remote Access Connection Manager
Remote Desktop Help Session Manager
Remote Registry
Routing and Remote access
Secondary logon
Simple Mail Transfer Protocol (SMTP)
Shell Hardware Detection
Smart Card
Special Administration Console Helper
TCP/IPNetBIOS Helper
Telephony
Telnet
Terminal Services Session Directory
Themes
Upload Manager
Web Client
Windows Audio
Windows Image Acquisition
WinHTTP Web Proxy Auto-discovery Service
Wireless Configuration

Internet Information Services IIS setup.

To stop the default FTP site, Web site and SMTP virtual server:
Expand the FTP Sites folder and right click on Default FTP Site, select stop.
Expand the Web Sites folder and right click on Default Web Site, select stop.
Right click on the Default SMTP Virtual Server and select stop

Change the default values for all websites before creation of new sites.
Right click and select properties for the "folder" WebSites.
At the Web Site tab, select properties for logging and change the logfile directory to the Data partition e.g. d:\logs.
The default for IIS is to store the logs under C:\WINDOWS\system32\LogFiles to store the logfiles under the system drive can cause problems if they grow quickly and are not deleted.

Home directory tab:
The only two that need to be checked are Read and Log visits.
Uncheck "Index this resource". If indexing needs to be turned on turn it on per website.
Make sure Directory Browsing is unchecked.
Under Application settings click on Configuration and select tab Option
Make sure that Enable parent paths is unchecked.
This is to make sure you can't traverse through the website.

Documents tab:
It is usually a good idea to add index.htm and index.html to the default content page list.

Change the default values for all ftpsites in IIS:
Right click and select properties for the "folder" FTP Sites.
In the tab "FTP site" select properties for logging and change the logfile directory to the Data partition, i.e. d:\logs.
In the Security Accounts Tab, make sure that Allow anonymous connections is not turned on.

In the "Home Directory", under FTP site directory select Read, Write and Log visits.

Before creating Any websites go to the Data drive and the folder you are going to have the websites under d:\domains. Right click and select properties then security settings for that folder and remove all users except administrator you might even have to add the administrator account and give it full permissions.

User Settings
Start->Administrative Tools-> Computer Management
Expand Local Users and Groups and go to Users.
In the Administrator account properties, under the Session tab:
Set End a disconnected session timeout to 5min.

After adding a user, make sure to disable remote desktop for that user.
Open up the properties box and under the General tab:
Uncheck User must change password at next logon.
Check User cannot change password.
Check Password never expires.

Note: If you don't have the following folders File and Printer sharing has been uninstalled

Environment tab:
Make sure all the boxes ar unchecked.
Remote Control tab:
Uncheck Enable remote control.
Terminal Services Profile tab:
Uncheck Allow logon to terminal server.

Change security settings for cmd.exe:
Right click on Start->explore go to c:\winnt\system32\.
Rightclick on cmd.exe select properties
Security tab:
Remove all users but the administrator which should have full permissions.

Change security settings for command.com:
Right click on Start->explore go to c:\winnt\system32\.
Rightclick on command.com select properties
Security tab:
Remove all users but the administrator which should have full permissions.

Enable Terminal Services for remote administration mode.
Click Start and select properties for My Computer.
At the bottom of the Remote tab.
Check Allow users to connect to this computer.

Final step:
Change the ip address, netmask, Default gateway and dns settings to the customer assigned, move it to the final location and make sure that you can connect to it with Remote Desktop.