1. **Configure a Security Policy:**

   Install Security Configuration Wizard through Add and remove windows components which detect ports and services, and configure registry and audit settings according to the server's role.

   - Disable unnecessary services based on the server role
   - Remove unused firewall rules and limit existing firewall rules.
   - Define restricted audit policies.

   For Configuring the Security Policy wizard Go to **Start --> Programs --> Administrative Tools --> Security Configuration Wizard.**
2. **Disable or Delete Unnecessary accounts:**

Attacks often gain access to servers through unused ports and services. So block the unused ports, protocols and by disabling services that are not required. During installation by default the Administrator, Guest and Help Assistant are created. As a security expertise the administrator account should be disabled to make it more difficult for an attacker to gain access. Both Guest and Help Assistant accounts should be disabled at all times.

For Disabling or deleting the accounts: Go to **Start --> programs --> Administrative Tools --> Server Manager Configuration --> Local Users and Groups --> users**

Right click on the user --> properties --> check for the account is disabled
3. **Uninstall Unnecessary applications or roles:**

   The number of applications installed on the servers should be role related. It is a good idea to test these applications out in a separate environment before deploying them on the production network. Some applications make use of service backdoors, which can sometimes compromise the overall security of the server.

   **Belarc Advisor:** It displays the installed software and hardware, missing patches fixes, antivirus status. It is free of cost and can be used for personal, government to look at their products which include many more features for managing security on multiple computers.

   For uninstalling the unnecessary application: Go to **start --> programs --> Administrative tools --> Server manager --> Roles --> Click remove roles**
4. **Configure the windows 2008 firewall:**

   Windows 2008 server comes with a built in firewall called the Windows Firewall with Advanced Security. As a security best practice, all servers should have its own host based firewall. Bi-directional firewall which filters the outbound traffic as well as inbound traffic. IPSEC encryption configurations are integrated into one interface. Using the advance rules you can build the firewall rules using Windows Active Directory objects, source & destination IP addresses and protocols.

   For configuring the windows 2008 firewall: Go to **Start --> Control Panel --> Windows Firewall --> Change Settings**
5. **Configure Auditing:**

The following events should be logged and audited.

- Audit account logon events
- Audit account management
- Audit directory service access
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

For Configuring the Auditing: Go to **Start** --> **Control Panel** --> **Administrative Tools** --> **Local Security policy** --> **Security Setting** --> **Local policies** --> **Audit policies**
6. **Disable Unnecessary shares:**

Unnecessary shares create a threat to critical servers. So it is necessary to disable the unnecessary shares. This can be done using the following command: `Net share`

This will display a list of all shares on the server. If there is a need to use a share, system and security administrators should configure the share as a hidden share and harden all NTFS and Share permissions.

C:\Documents and Settings>net share

<table>
<thead>
<tr>
<th>Share name</th>
<th>Resource</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMIN$</td>
<td>C:\WINDOWS</td>
<td>Remote Admin</td>
</tr>
<tr>
<td>C$</td>
<td>C:\</td>
<td>Default share</td>
</tr>
<tr>
<td>IPC$</td>
<td>C:\</td>
<td>Remote IPC</td>
</tr>
</tbody>
</table>

In order to create a hidden share, put a $ (Dollar) sign after the share name. The share will still be accessible; however it will not be easily listed through the network. Example: Accounting$
7. **Configure Encryption:**

According to industry standards, the servers require host sensitive information to make use of the encryption system. Windows Server 2008 provides a built in whole disk encryption feature called BitLocker Drive Encryption (BitLocker) which protects the operating system and data stored on the disk. To install BitLocker, select it in Server Manager or type the following at a command prompt:

```
C:\ServerManagerCmd -install BitLocker -restart
```

For Configuring the Encryption on 2008 server: Go to Start --> Programs --> Administrative Tools --> Server Manager --> Features --> Bit locker (It will be accessed only when active directory gets installed in windows server 2008)

8. **Updates and Patches:**

Updates and Patches are key elements for hardening a server. The system and security expertise should be constantly updating and patching their servers against vulnerabilities. Administrators should periodically check the vendor's websites for updates. Windows Server Update Services (WSUS) provides a software update service for Microsoft Windows operating systems and other Microsoft software.

For updating Go to: Start --> Windows Update (Make sure Automatic Updates is turned ON)
9. **Antivirus and Network Access Point (NAP):**

Anti Virus software is one of the basic and crucial step for hardening a server. Windows Server 2008 comes with a Network Access Protection (NAP) which helps to defense against viruses from spreading out into the network.

It uses a set of policies which cleans the affected machines and when they are healthy, permits them access to parts of the production network. NAP consists of client server technology which scans and identifies machines that don't have the latest virus signatures, service packs or security patches.

For updating the Antivirus Go to: [http://www.microsoft.com/security/default.aspx](http://www.microsoft.com/security/default.aspx)
10. **Least Privilege:**

Most of the security threats are often caused by high privileges bared by accounts. Server services should not be configured using enterprise wide administrator accounts. Script Logic Cloak is a product which enhances the Windows NT File System (NTFS) by providing increased security, more accurate audits.

For Least Privilege: Download **Script Logic Cloak** and install in your windows 2008 server which enchance the Windows NT file system Secuirty
11. Disable Automatic Services:

Here are all the services are disabled that were set to automatic startup. By disabling these services you can limit attack surface area which can prevent or limit exploitation of the server.

For Disable Automatic services Go to: **Start --> run --> Services.msc --> Disable unneeded services**
12. **Disable Remote Registry:**

This service allows registry access to authenticated remote users. Even though this is blocked by the firewall and ACLs this service should be turned off if you have no reason to allow remote registry access.

For Disabling the remote registry Go to: **Start --> Control Panel --> Windows firewall --> ON**

If you have Corporate network follow the below steps:

**Click Start – RUN --> Type "regedit" and press enter --> Navigate to**

**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\**

Select "winreg" and click Edit, Select "Permissions"

Select appropriate users/groups & appropriate permission like "Read" or "full Control". Click OK and exit.

13. **Windows Error Reporting Service:**

Windows Error Reporting (WER) is a set of Windows technologies that capture software crash data and support end-user reporting of crash information. Through Winqual services, software and hardware vendors can access reports in order to analyze and respond to these problems. WER technologies are implemented in Windows XP, Windows Server 2003, and later.

Go to: **Start --> programs --> Administrative tools --> server manager --> Configuration --> Local users and groups.**
14. **Enable Web management Service:**

Enables remote management of the web server, sites, and applications on this machine. The primary goal of enterprises that are currently using Web Services is to derive a business sense out of this technology and drive their strategies based on that. This can only be done when they have proper control over Web Services offered to their customers.

For Enabling Web Management Service Go to: **Start -> programs --> Administrative Tools --> Server manager --> Roles --> Add roles --> Check for IIS --> Management Tools --> Check for Management service.**
15. **Use Secure Socket Tunnelling protocol (SSTP) Service:**

Provides support for the Secure Socket Tunneling Protocol (SSTP) to connect to remote computers using VPN. If this service is disabled, users will not be able to use SSTP to access remote servers.

SSTP allows traffic to pass through firewalls that block PPTP and L2TP/IPsec traffic. It encapsulates PPP traffic over the SSL channel of the HTTPS protocol (Port 443). It allows clients behind firewalls and NAT routers to connect to the VPN server without the concern for typical port blocking issues.

For using the SSTP service Go to: `start --> run --> services.msc --> secure socket tunnelling`
16. **Certificate Propagation:**

Smart Card certificate handling. Microsoft has included many smart-card services in Vista, but probably not too many people use them. Do not get these confused with memory cards, they are completely different things. Smart-cards are used sometimes for logging into vista instead of a password.

For Certificate Propagation Go to: **Start --> run --> services.msc --> certificate propagation --> Automatic**
17. **Enable NetLogon:**

Maintains a channel between computer and domain controller. The Netlogon sub-key stores information for the Net Log-on service. The Net Log on service verifies log-on requests, and it registers, authenticates, and locates domain controllers. Also, to maintain backward compatibility, Net Log-on manages replication of the user account database to back up domain controllers running Windows NT 4.0 and earlier.

For Enabling Netlogon Go to: **Start --> run--> services.msc --> Netlogon --> Automatic**

18. **Special Administration Console Helper:**

Allows administrators to remotely access a command prompt. The Special Administration Console (SAC) can connect to a machine, where this service is running. SAC can perform remote management tasks in case Windows on the machine stops functioning due to a Stop error message.

The SAC is an auxiliary Emergency Management Services command-line environment with the
Following main functions:

- Redirect Stop error message explanatory text.
- Restart the system.
- Obtain computer identification information.

Go to: **Start --> run --> Services.msc --> special administration console helper --> Automatic**